Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1-20. (cancelled)

21. (currently amended) A system comprising:

a network;

~~a security operation center coupled with the network;~~ and

one or more machines coupled with the network, each machine comprising a communication interface and a memory including an execution area configured to perform operations ~~comprising examining~~ to examine a set of instructions embodying an invoked application to identify the invoked application, obtain~~ing~~ application-specific intrusion criteria, the application-specific intrusion criteria including intrusion signatures and behavior criteria, and monitor~~ing~~ network communications for the invoked application~~, after the examining and the obtaining, using the~~ for application-specific intrusion signatures and abnormal application behavior ~~criteria~~ to detect an intrusion.

22. (original) The system of claim 21, wherein the application-specific intrusion criteria comprises a normal communication behavior threshold.

23. (cancelled)

24. (currently amended) The system of claim 21, wherein to monitor~~ing~~ network communications comprises to monitor~~ing~~ network communications in a network intrusion detection system component running in an execution context with the invoked application.

25. (currently amended) The system of claim 24, wherein the operations further comprise to ~~providing~~ provide an application-specific remedy for a detected intrusion.

26. (currently amended) The system of claim 25, wherein to provide ~~providing~~ an application-specific remedy comprises cutting at least a portion of the network communications for the invoked application.

27. (currently amended) The system of claim 24, wherein each machine further comprises a local repository and a security operation center, the security operation center includes a master repository, and wherein to obtain~~ing~~ the application-specific intrusion criteria comprises to:

request~~ing~~ the application-specific intrusion criteria from the local repository;

request~~ing~~ the application-specific intrusion criteria from the master repository if the application-specific intrusion criteria is unavailable in the local repository;

~~receiving~~ receive the application-specific intrusion criteria from the master repository if requested; and

~~receiving~~ receive the application-specific intrusion criteria from the local repository.

28. (currently amended) The system of claim 24, wherein to examine ~~examining~~ the set of instructions comprises to:

apply~~ing~~ a hash function to the set of instructions to generate a condensed representation; and

~~comparing~~ compare the condensed representation with existing condensed representations for known applications.

29-30. (cancelled)

31. (new) A detection method, comprising:

examining a set of instructions embodying an invoked application to identify the invoked application;

obtaining application-specific intrusion criteria, the application-specific intrusion criteria including application-specific intrusion signatures and behavior criteria; and

monitoring network communications for the invoked application for application-specific intrusion signatures and abnormal application behavior to detect an intrusion.

32. (new) The method of claim 31, wherein examining a set of instructions embodying an invoked application to identify the invoked application comprises:

applying a hash function to the set of instructions to generate a condensed representation; and

comparing the condensed representation with existing condensed representations for known applications.

33. (new) The method of claim 31, wherein network communications are monitored for application-specific intrusion signatures that correspond to the identified invoked application.

34. (new) The method of claim 31, further comprising unloading the application-specific intrusion signatures corresponding to the identified invoked application when the identified invoked application is terminated.

35. (new) The method of claim 31, further comprising tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

36. (new) The method of claim 35, wherein tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds.

37. (new) The method of claim 35, wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

38. (new) The method of claim 37, wherein the network intrusion detection system component and the invoked application run within a single execution context.

39. (new) The method of claim 31, further comprising operations to provide an application-specific remedy for a detected intrusion.

40. (new) The method of claim 39, wherein operations to provide an application-specific remedy for a detected intrusion comprises cutting at least a portion of the network communications for the invoked application and/or notifying a system administrator of the identified application-specific abnormal communication behavior.

41. (new) The method of claim 31, wherein obtaining the application-specific intrusion detection signature comprises loading the application-specific intrusion detection signature from a local signature repository.

42. (new) The method of claim 31, wherein obtaining the application-specific intrusion detection signature comprises:

requesting the application-specific intrusion detection signature from a local signature repository in communication with a remote signature repository; and

receiving the application-specific intrusion detection signature from the local signature repository.

43. (new) A machine-readable storage medium embodying machine instructions for causing one or more processors to perform operations comprising:

examining a set of instructions embodying an invoked application to identify the invoked application;

obtaining application-specific intrusion criteria, the application-specific intrusion criteria including application-specific intrusion signatures and behavior criteria; and

monitoring network communications for the invoked application for application-specific intrusion signatures and abnormal application behavior to detect an intrusion.

44. (new) The machine-readable storage medium of claim 43, wherein examining a set of instructions embodying an invoked application to identify the invoked application comprises:

applying a hash function to the set of instructions to generate a condensed representation; and

comparing the condensed representation with existing condensed representations for known applications.

45. (new) The machine-readable storage medium of claim 43, wherein network communications are monitored for application-specific intrusion signatures that correspond to the identified invoked application.

46. (new) The machine-readable storage medium of claim 43, further comprising unloading the application-specific intrusion signatures corresponding to the identified invoked application when the identified invoked application is terminated.

47. (new) The machine-readable storage medium of claim 43, further comprising tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

48. (new) The machine-readable storage medium of claim 47, wherein tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds.

49. (new) The machine-readable storage medium of claim 47, wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

50. (new) The machine-readable storage medium of claim 49, wherein the network intrusion detection system component and the invoked application run within a single execution context.

51. (new) The machine-readable storage medium of claim 43, further comprising operations to provide an application-specific remedy for a detected intrusion.